Initialization of a chip card

Publication number: DE10142351
Publication date: 2003-03-20
Inventor: HARTEL KARL EGLOF (DE); VATER HARALD (DE)
Applicant: GIESECKE & DEVRIENT GMBH (DE)
Classification:
- international: ***G07F7/10;*** **G07F7/10;** (IPC1-7): G06K19/073;¡G06F12/14
- european: G07F7/10; G07F7/10D2; G07F7/10D2K
Application number: DE20011042351 20010830
Priority number(s): DE20011042351 20010830

Also published as:
WO03021542 (A1)
EP1425723 (A1)
US2005120226 (A1)
EP1425723 (A0)
CN1561507 (A)

more >>

Abstract of **DE10142351**

The invention relates to a method for reading initialization data (IND) into a chip card, according to which the chip card receives an encrypted authentication value (EAV) and decrypts the same in order to receive at least one enable key (ENK). Said enable key (ENK) is checked for its concordance with an enable key (ENK') stored on the chip card (14). If the keys concord, the initialization data (EIND, IND) are received and written into a non-volatile memory of the chip card. The invention also relates to a method for producing a data record used for the initialization of a chip card, according to which the chip card and a computer-readable data carrier have matching features. The invention is especially provided for the initialization of chip cards by external partners of the chip card producer, and is especially tamper-proof.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 42 351 A 1**

(51) Int. Cl.[7]:
G 06 K 19/073
G 06 F 12/14

(21) Aktenzeichen: 101 42 351.9
(22) Anmeldetag: 30. 8. 2001
(43) Offenlegungstag: 20. 3. 2003

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Hartel, Karl Eglof, 80687 München, DE; Vater, Harald, Dr., 35398 Gießen, DE

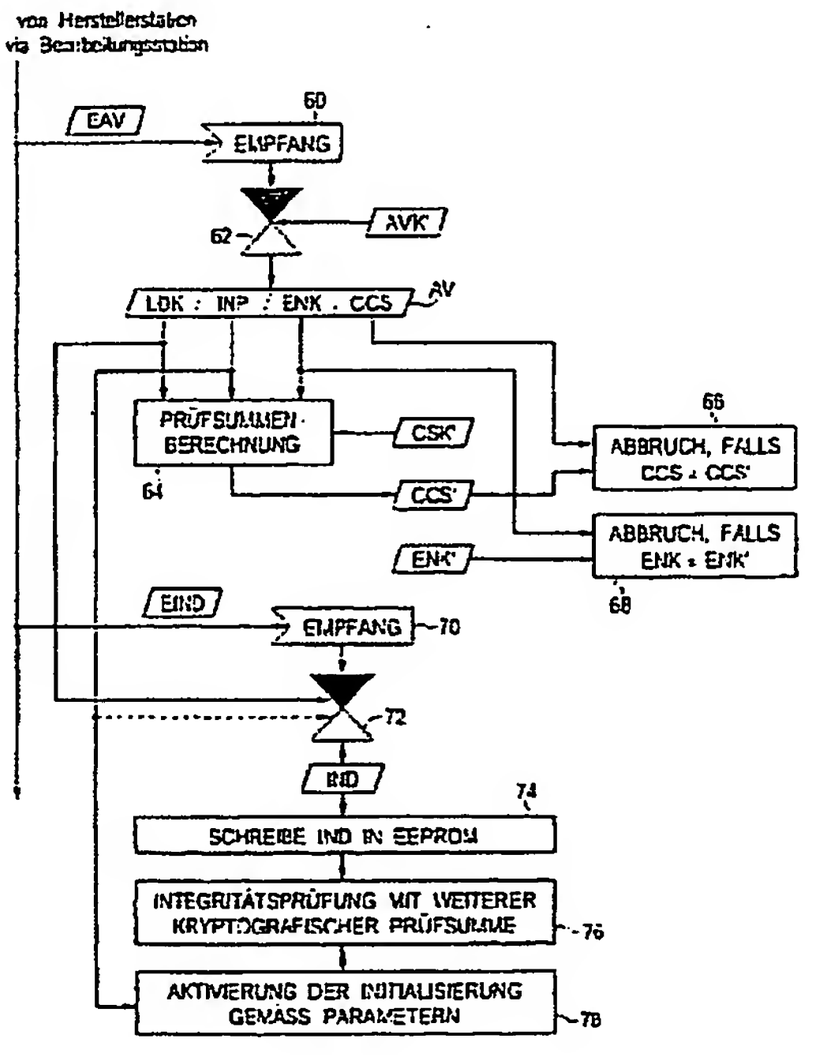
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 198 22 217 A1
DE 195 17 818 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Initialisieren einer Chipkarte

(57) Bei einem Verfahren zum Einlesen von Initialisierungsdaten (IND) in eine Chipkarte empfängt die Chipkarte einen verschlüsselten Authentisierungswert (EAV) und entschlüsselt diesen, um zumindest einen Freigabeschlüssel (ENK) zu erhalten. Der Freigabeschlüssel (ENK) wird auf Übereinstimmung mit einem auf der Chipkarte (14) gespeicherten Freigabeschlüssel (ENK') überprüft. Falls eine Übereinstimmung vorliegt, werden die Initialisierungsdaten (EIND, IND) empfangen und in einen nichtflüchtigen Speicher der Chipkarte eingeschrieben. Ein Verfahren zum Erzeugen eines Datensatzes für die Initialisierung einer Chipkarte, eine Chipkarte und ein computerlesbarer Datenträger weisen korrespondierende Merkmale auf. Die Erfindung ist insbesondere für die Initialisierung von Chipkarten durch externe Partner des Chipkartenherstellers vorgesehen, wobei möglichst wenige Angriffsmöglichkeiten geboten werden sollen.



DE 101 42 351 A 1

Beschreibung

[0001] Die Erfindung betrifft das technische Gebiet der Initialisierung einer Chipkarte und insbesondere die Zusammenstellung und Verarbeitung eines Datensatzes, der bei einem Initialisierungsschritt in die Chipkarte eingelesen wird.

[0002] Chipkarten sind in vielerlei Ausgestaltungen gut bekannt. Sie werden beispielsweise zur Zugangskontrolle oder im Zahlungsverkehr eingesetzt und weisen in der Regel einen Halbleiterchip mit einem Mikrocontroller und mindestens einem Speicher auf. Neben den üblichen Bauformen in Scheckkartengröße oder als kleine Kartenmodule (z. B. SIMs – subscriber identity modules bei Mobiltelefonen) werden Chipkarten auch in anderen Bauformen (z. B. als Schlüsselanhänger oder Ringe) hergestellt. Alle diese Ausgestaltungen sollen im vorliegenden Text mit dem Begriff "Chipkarte" bezeichnet werden.

[0003] Bei der Herstellung von Chipkarten ist die Initialisierung derjenige Verfahrensschritt, bei dem nach der Fertigstellung und dem erfolgreichen Test der Chipkartenhardware solche Programme und/oder Daten in die Chipkarte eingespielt werden, die für eine größere Anzahl von Chipkarten identisch sind. Der daran anschließende Schritt des Ladens von personenbezogenen, individuellen Daten wird als Personalisierung bezeichnet.

[0004] Die Trennung der beiden genannten Schritte erfolgt aus fertigungstechnischen Gründen, um die Menge der individuell in einzelne Chipkarten zu übertragenden Daten möglichst gering zu halten. In manchen Anwendungsfällen ist zwischen die Schritte der Initialisierung und der Personalisierung noch die sogenannte Nachinitialisierung geschaltet, bei der zusätzliche Programme und/oder Daten in eine relativ kleine Anzahl von Chipkarten eingeschrieben werden. Ein Überblick über diese Herstellungsschritte und deren Abgrenzung ist in Kapitel 10.4 (Seiten 584 bis 592) des Buches "Handbuch der Chipkarten" von Wolfgang Rankl und Wolfgang Effing, 3. Auflage 1999, enthalten.

[0005] Nach einem zumindest firmeninternen Stand der Technik der Anmelderin ist in Chipkarten für das GSM-Mobiltelefonsystem ein 32 Byte langer Freigabeschlüssel in einem maskenprogrammierten ROM der Chipkarte enthalten. Zum Starten des Initialisierungsvorgangs muß ein zum Freigabeschlüssel passender Datenwert mit einem geeigneten Kommando (z. B. VERIFY INITIALISATION KEY) an die Chipkarte übergeben werden. Der übergebene Wert wird mit dem im Chipkarten-ROM gespeicherten Freigabeschlüssel verglichen. Bei einer Übereinstimmung wird der Zugriff auf ein EEPROM der Chipkarte und auf alle für die Initialisierung benötigten Chipkartenkommandos freigegeben.

[0006] Das darauffolgende Laden der Initialisierungsdaten in die Chipkarte kann entweder offen oder mit einem Ladeschlüssel verschlüsselt erfolgen. Durch das verschlüsselte Laden wird sichergestellt, daß auch bei einem unbefugten Zugriff auf die verschlüsselten Initialisierungsdaten deren Vertraulichkeit gewahrt bleibt.

[0007] Bei diesem System besteht jedoch nach wie vor das Problem, daß der Freigabeschlüssel derjenigen Stelle, die die Initialisierung durchführt, bekannt sein muß. Zunehmend wird gefordert, daß nicht der Chipkartenhersteller selber, sondern externe Partner (z. B. Mobiltelefon-Netzbetreiber) die Chipkarten in eigener Regie initialisieren. Es besteht in diesem Fall die Gefahr, daß der Freigabeschlüssel bei der Übermittlung zu dem externen Partner oder beim Einlesen in die Chipkarte ausgespäht wird, oder daß der externe Partner den Freigabeschlüssel nicht streng geheimhält.

[0008] Wenn der Freigabeschlüssel unberechtigten Personen zugänglich gemacht werden würde, könnte möglicherweise eine ganze Chipkarten-Produktlinie kompromittiert werden, weil der Freigabeschlüssel Zugriff zu diversen grundlegenden Chipkartenfunktionen ermöglicht, die ihrerseits zum Ausspähen der Hard- und Software der Chipkarte eingesetzt werden können. Beispielsweise könnte bei Kenntnis des Freigabeschlüssels ein unberechtigter Dritter einen eigenen Programmcode in die Chipkarte laden und damit den bereits im maskenprogrammierten ROM befindlichen Code ausspähen.

[0009] Aus der deutschen Offenlegungsschrift DE 196 33 466 A1 ist ein Verfahren zur Nachinitialisierung von Chipkarten bekannt. Bei diesem Verfahren wird, ähnlich der oben im Zusammenhang mit der Initialisierung beschriebenen Vorgehensweise, ein Schlüssel zur Freigabe bestimmter Kommandos des Chipkarten-Betriebssystems verwendet.

[0010] Die deutsche Offenlegungsschrift DE 199 02 722 A1 zeigt ein kryptographisches Verfahren zum Austauschen eines geheimen Anfangswerts zwischen einer Bearbeitungsstation und einer Chipkarte, bei dem eine Übermittlung des Anfangswerts im Klartext vermieden wird.

[0011] Aufgabe der Erfindung ist es, die genannten Probleme zumindest zum Teil zu vermeiden und eine Möglichkeit zur Initialisierung von Chipkarten bereitzustellen, die sich insbesondere für die Durchführung der Initialisierung durch externe Partner eignet und dabei nur wenige oder keine Angriffsmöglichkeiten bietet. Insbesondere soll das Risiko vermindert werden, daß ein Unbefugter Zugriff auf die geschützten Initialisierungskommandos erhält und/oder ein unbefugtes Laden von Programmcodes in die Chipkarte erfolgt.

[0012] Zur Lösung dieser Aufgabe sind erfindungsgemäße Verfahren und Vorrichtungen mit den Merkmalen der unabhängigen Ansprüche vorgesehen. Die abhängigen Ansprüche definieren bevorzugte Ausgestaltungen der Erfindung.

[0013] Anspruch 1 definiert die von der Chipkarte beim Einlesen des Initialisierungs-Datensatzes ausgeführten Schritte. Anspruch 5 betrifft eine Chipkarte, die zum Ausführen dieser Schritte ausgestaltet ist. Anspruch 6 definiert das vom Chipkartenhersteller ausgeführte Verfahren, um einen geeigneten Datensatz zur Ausführung der erfindungsgemäßen Chipkarteninitialisierung, zu erhalten. Anspruch 10 betrifft einen computerlesbaren Datenträger mit einem derartigen Datensatz. Anspruch 11 betrifft das erfindungsgemäße Gesamtverfahren, das im wesentlichen aus den zwei "spiegelbildlichen" Abschnitten des Erzeugens und des Auswertens des Initialisierungs-Datensatzes zusammengesetzt ist.

[0014] Die Erfindung beruht auf der Grundidee, den Freigabeschlüssel weder im Klartext dem externen Partner zugänglich zu machen noch ihn im Klartext an die Chipkarte zu übertragen. Vielmehr wird der Freigabeschlüssel (gegebenenfalls zusammen mit weiteren Informationen) in einen Authentisierungswert aufgenommen, und der Authentisierungswert wird ausschließlich in verschlüsseltem Zustand vom Hersteller zum externen Partner und von einer Bearbeitungsstation des externen Partners zur Chipkarte übertragen.

[0015] Die Erfindung bietet erhebliche Vorteile dadurch, daß der Freigabeschlüssel im Klartext weder an den externen Partner noch an die Chipkarte übertragen wird und auch dem externen Partner nicht zugänglich ist. Dadurch wird ein unbefugter Zugang zu den Initialisierungskommandos der Chipkarte zuverlässig vermieden.

[0016] Die Sicherheit des gesamten Chipkartensystems, die auch auf der sicheren Geheimhaltung der internen Strukturen und internen Programmierung der Chipkarte beruht, wird damit erhöht, während gleichzeitig externen Partnern

die Möglichkeit gegeben wird, Initialisierungsvorgänge im eigenen Hause auszuführen. Dies vergrößert die Akzeptanz des Chipkartensystems z. B. bei GSM-Netzbetreibern und erweitert den möglichen Anwendungsbereich von Chipkarten auch auf Einsatzgebiete, bei denen eine externe Initialisierung der Chipkarte erforderlich oder wünschenswert ist.

[0017] Die Aufzählungsreihenfolge der Schritte in den Ansprüchen soll nicht einschränkend aufgefaßt werden. Es sind vielmehr Ausführungsformen der Erfindung vorgesehen, in denen diese Schritte in anderer Reihenfolge oder parallel oder quasi-parallel (ineinander verzahnt) ausgeführt werden.

[0018] Als "computerlesbarer Datenträger" im hier verwendeten Sinne sollen nicht nur materielle Datenträger, wie beispielsweise magnetische oder optische Platten oder Bänder, sondern auch immaterielle Datenträger, wie beispielsweise Spannungssignale oder optische Signale, mit aufmodulierten Dateninformationen verstanden werden.

[0019] In der Wortwahl des vorliegenden Textes soll mit dem Begriff "Initialisierung" vorzugsweise die eingangs genannte Übertragung von Programmen und Daten in eine größere Anzahl von Chipkarten verstanden werden. In anderen Ausgestaltungen der Erfindung ist der Begriff "Initialisierung" jedoch weiter aufzufassen und umfaßt neben der Initialisierung im engeren Sinne auch eine Nachinitialisierung und/oder eine Personalisierung. Als "Initialisierungsdaten" werden im vorliegenden Text nicht nur Daten im engeren Sinne, sondern auch Programme, Programmfragmente und Befehle bezeichnet.

[0020] Erfindungsgemäß wird eine Übereinstimmung eines empfangenen Freigabeschlüssels mit einem auf der Chipkarte gespeicherten Freigabeschlüssel überprüft. Unter dem Begriff "Übereinstimmung" ist hierbei vorzugsweise eine Identität der beiden Freigabeschlüssel zu verstehen. In anderen Ausführungsformen der Erfindung kann jedoch auch eine andere Beziehung zwischen den beiden Freigabeschlüsseln gefordert werden. Diese andere Beziehung (z. B., daß die beiden Freigabeschlüssel zueinander komplementär sind) wird in diesen Ausführungsformen als "Übereinstimmung" bezeichnet. Wenn die Übereinstimmung festgestellt wurde, werden die Initialisierungsdaten in einen Speicher, vorzugsweise ein EEPROM oder ein nichtflüchtiges RAM, eingeschrieben.

[0021] In bevorzugten Ausführungsformen der Erfindung ist vorgesehen, daß die Initialisierungsdaten nicht im Klartext, sondern als verschlüsselte Initialisierungsdaten übertragen werden. Die zur Entschlüsselung erforderlichen Informationen sind in dem Authentisierungswert enthalten oder aus diesem ableitbar. Diese Informationen können insbesondere ein Ladeschlüssel zur Entschlüsselung der verschlüsselten Initialisierungsdaten sein. Die verschlüsselte Übertragung der Initialisierungsdaten hat den Vorteil, daß die in diesen Initialisierungsdaten enthaltenen Betriebsgeheimnisse des Chipkartenherstellers sicher gewahrt bleiben. Überdies wird eine gezielte Verfälschung der Initialisierungsdaten noch weiter erschwert.

[0022] In bevorzugten Ausgestaltungen der Erfindung beeinflussen ein oder mehrere Initialisierungsparameter, die im Authentisierungswert enthalten sind, das Laden der Initialisierungsdaten (z. B., indem eines von mehreren möglichen Verschlüsselungsverfahren eingestellt wird). Alternativ oder zusätzlich ist in weiteren Ausgestaltungen der Erfindung vorgesehen, daß die Initialisierungsparameter den weiteren Ablauf der Initialisierung und/oder die spätere Funktionsweise der Chipkarte beeinflussen. Beispielsweise kann durch die Initialisierungsparameter eine Auswahl zwischen mehreren, im maskenprogrammierten ROM der Chipkarte befindlichen Algorithmen für bestimmte, spätere Funktionen der Chipkarte getroffen werden. Durch diese Ausgestaltung vergrößert sich der Anwendungsbereich der Erfindung nochmals erheblich.

[0023] Um den Authentisierungswert gegen unbefugte Manipulationen zu schützen, ist in bevorzugten Ausgestaltungen der Erfindung entweder der gesamte Authentisierungswert oder einzelne Teile davon (der Freigabeschlüssel und/oder der Ladeschlüssel und/oder die Initialisierungsparameter) durch eine kryptographische Prüfsumme abgesichert.

[0024] In bevorzugten Ausgestaltungen der erfindungsgemäßen Verfahren sowie der erfindungsgemäßen Chipkarte und des erfindungsgemäßen Datenträgers weisen diese Merkmale auf, die den oben beschriebenen oder den in den abhängigen Ansprüchen definierten Merkmalen entsprechen.

[0025] Weitere Merkmale, Eigenschaften und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung eines Ausführungsbeispiels und mehrerer Ausführungsalternativen. In den schematischen Zeichnungen zeigen:

[0026] **Fig. 1** eine Übersicht über die an dem Gesamtverfahren beteiligten Komponenten und Datenkommunikationswege,

[0027] **Fig. 2** ein Datenflußdiagramm des Verfahrens zum Erstellen des zur Chipkarteninitialisierung verwendeten Datensatzes und

[0028] **Fig. 3** ein Datenflußdiagramm des von der Chipkarte ausgeführten Verfahrens bei der Initialisierung.

[0029] In **Fig. 1** sind schematisch eine Herstellerstation **10**, eine Bearbeitungsstation **12** und eine Chipkarte **14** gezeigt. Die Herstellerstation **10** ist beim Hersteller der Chipkarte **14** angeordnet, während die Bearbeitungsstation **12** und die Chipkarte **14** sich bei einem externen Partner des Chipkartenherstellers befinden. Zwischen der Herstellerstation **10** und der Bearbeitungsstation **12** besteht eine Datenübertragungsstrecke **16**, die beispielsweise als elektronischer Kommunikationsweg über eine Telefonleitung oder auch durch den Austausch von Datenträgern verwirklicht sein kann. Die Chipkarte **14** ist über eine Leitungsverbindung **18** an die Bearbeitungsstation **12** angeschlossen.

[0030] Bestandteile der Chipkarte **14** sind ein Halbleiterchip **20** sowie ein Kontaktfeld **22**, dessen Kontakte an die Leitungsverbindung **18** angeschlossen sind. Der Halbleiterchip **20** weist in an sich bekannter Weise eine Schnittstellenschaltung **24**, einen Mikrocontroller **26**, einen Schreib-/Lese-Speicher **28** (RAM = random access memory), einen nicht-flüchtigen Speicher **30** und einen maskenprogrammierten Festwertspeicher **32** (ROM = read only memory) auf. Der nicht-flüchtige Speicher **30** ist im vorliegenden Ausführungsbeispiel als elektrisch löschbarer Speicher (EEPROM = electrically erasable read only memory) ausgestaltet. Die genannten Funktionsblöcke des Halbleiterchips **20** sind untereinander durch einen Bus **34** verbunden. Die Schnittstellenschaltung **24** ist überdies an das Kontaktfeld **22** angeschlossen.

[0031] Die bisher beschriebene Ausgestaltung der Chipkarte **14** ist an sich bekannt. Es ist ebenfalls bekannt, daß der Festwertspeicher **32** einen vorgegebenen Freigabeschlüssel ENK' aufweist. Die in **Fig. 1** gezeigte Chipkarte **14** unterscheidet sich jedoch dadurch vom Stand der Technik, daß ferner ein Prüfsummenschlüssel CSK' und ein Authentisierungswertschlüssel AVK' im maskenprogrammierten Festwertspeicher **32** der Chipkarte **14** vorgesehen sind. Der Authentisierungswertschlüssel AVK dient zur Entschlüsselung eines unten noch im Detail beschriebenen Authentisierungswertes, während der Prüfsummenschlüssel CSK' zur Integritätsprüfung dieses Authentisierungswertes vorgesehen ist.

[0032] Die Herstellerstation **10** hat Zugriff auf die beim

Initialisierungsvorgang in die Chipkarte **14** zu übertragenden Initialisierungsdaten IND, die in der Regel sowohl Programmbefehle als auch Datenwerte enthalten. Ferner liegen in der Herstellerstation **10** ein oder mehrere Initialisierungsparameter INP sowie eine Kennung des externen Partners EXT vor. Schließlich weist die Herstellerstation **10** auch Datenwerte für einen Freigabeschlüssel ENK, einen Prüfsummenschlüssel CSK und einen Authentisierungswertschlüssel AVK auf. Diese Werte ENK, CSK und AVK sind identisch zu den in der Chipkarte **14** gespeicherten Werten ENK', CSK' und AVK'.

[0033] Bei dem Zusammenstellen eines für die Initialisierung benötigten Datensatzes DS führt die Herstellerstation **10** ein Verfahren aus, das in **Fig. 2** gezeigt ist und unten noch genauer beschrieben werden wird. Das Ergebnis dieses Verfahrens ist, daß der Datensatz DS verschlüsselte Initialisierungsdaten EIND und einen verschlüsselten Authentisierungswert EAV aufweist. Dieser Datensatz DS wird zur Bearbeitungsstation **12** übertragen und dort zwischengespeichert. Bei der Initialisierung der Chipkarte **14** überträgt die Bearbeitungsstation **12** den Datensatz DS zur Chipkarte **14**. Dort werden die empfangenen Daten nach dem in **Fig. 3** gezeigten Verfahren ausgewertet, das ebenfalls unten genauer beschrieben wird.

[0034] Das Verfahren gemäß **Fig. 2** wird von der Herstellerstation **10** ausgeführt. Es geht von den vorgegebenen Initialisierungsdaten IND aus. Aus diesen Daten und der Kennung des externen Partners EXT wird in Schritt **40** ein Ladeschlüssel LDK erzeugt. Im hier beschriebenen Ausführungsbeispiel ist der Ladeschlüssel LDK ein Zufallswert, der für jedes Paar der Werte IND, EXT neu generiert wird. In Ausführungsalternativen kann der Ladeschlüssel LDK in Schritt **40** auch nach einem anderen Verfahren berechnet werden.

[0035] Der Ladeschlüssel LDK erfüllt mehrere Funktionen. Er dient erstens zur Verschlüsselung der Initialisierungsdaten IND in Schritt **42**, um verschlüsselte Initialisierungsdaten EIND zu erhalten. Zweitens ist der Ladeschlüssel LDK eine Komponente eines Authentifizierungswertes AV. Weitere Komponenten des Authentifizierungswertes AV sind ein oder mehrere Initialisierungsparameter INP sowie der Freigabeschlüssel ENK.

[0036] Im hier beschriebenen Ausführungsbeispiel wird ferner aus den genannten drei Werten LDK, INP und ENK in Schritt **44** eine kryptographische Prüfsumme CCS berechnet, wobei der Prüfsummenschlüssel CSK als Schlüssel herangezogen wird. Als Algorithmus zur Prüfsummenberechnung wird im vorliegenden Ausführungsbeispiel ein an sich bekannter MAC (message authentication code; siehe Kapitel 4.6.4 des bereits zitierten Buches "Handbuch der Chipkarten") nach ISO 9797 eingesetzt, während in Ausführungsalternativen andere Berechnungsverfahren vorgesehen sind. Die kryptographische Prüfsumme CCS sichert die Integrität der im Authentisierungswert AV enthaltenen Daten.

[0037] Im hier beschriebenen Ausführungsbeispiel ist der Authentisierungswert AV die Konkatenation der Werte LDK, INP, ENK und der kryptographischen Prüfsumme CCS, während in Ausführungsalternativen andere Verfahren zur Bestimmung des Authentisierungswerts AV eingesetzt werden und der Authentisierungswert AV weitere und/oder andere und/oder weniger Daten enthalten kann.

[0038] In einem weiteren Verschlüsselungsschritt **46** wird der Authentisierungswert AV mit dem Authentisierungswertschlüssel AVK verschlüsselt, um einen verschlüsselten Authentisierungswert EAV zu erhalten. Als Verschlüsselungsverfahren kann in Schritt **46** beispielsweise eines der an sich bekannten Verfahren DES (data encryption standard; siehe Kapitel 4.6.1 des bereits zitierten Buches "Handbuch der Chipkarten") oder TRIPLE DES eingesetzt werden, und zwar bevorzugt im CBC-Modus (cipher block chaining), weil durch diesen Modus die internen Strukturen des Authentisierungswerts AV verborgen werden. In Ausführungsalternativen sind dagegen andere Verschlüsselungsverfahren für Schritt **46** vorgesehen.

[0039] In den beiden abschließenden Verfahrensschritten **48** und **50** werden zunächst der verschlüsselte Authentisierungswert EAV und dann die verschlüsselten Initialisierungsdaten EIND an die Bearbeitungsstation **12** gesendet, um dort zwischengespeichert und schließlich an die Chipkarte **14** geleitet zu werden. Die genannten, verschlüsselten Daten EAV und EIND bilden zusammen den in **Fig. 1** gezeigten Datensatz DS, der in Ausführungsalternativen weitere Komponenten enthalten kann.

[0040] **Fig. 3** betrifft den Empfang und die Verarbeitung des Datensatzes DS (**Fig. 1**) durch die Chipkarte **14**. In Schritt **60** empfängt die Chipkarte **14** zunächst den verschlüsselten Authentisierungswert EAV, der ursprünglich von der Herstellerstation **10** stammt und an die Bearbeitungsstation **12** übertragen wurde. Der verschlüsselte Authentisierungswert EAV wird in Schritt **62** mit dem im Festwertspeicher **32** der Chipkarte **14** abgelegten Authentisierungswertschlüssel AVK' entschlüsselt, um den Authentisierungswert AV mit den Komponenten LDK, INP, ENK und CCS zu erhalten. Zur Vereinfachung der vorliegenden Beschreibung soll davon ausgegangen werden, daß keine Verfälschung des Datensatzes DS stattgefunden hat, weshalb der in Schritt **62** berechnete Authentisierungswert AV identisch mit dem in **Fig. 2** gezeigten Authentisierungswert AV ist.

[0041] Wiederum erfolgt eine Prüfsummenberechnung (Schritt **64**), bei der aus den Komponenten LDK, INP und ENK unter Verwendung des in der Chipkarte **14** gespeicherten Prüfsummenschlüssels CSK' eine kryptographische Prüfsumme CCS' ermittelt wird. Der Authentisierungswert AV wird als fehlerhaft verworfen, und das Verfahren wird abgebrochen, falls in Schritt **66** eine Abweichung der berechneten Prüfsumme CCS' von der im entschlüsselten Authentisierungswert AV enthaltenen Prüfsumme CCS festgestellt wird.

[0042] War die Prüfsummenberechnung erfolgreich, so wird in einem weiteren Schritt **68** der im entschlüsselten Authentisierungswert AV enthaltene Freigabeschlüssel ENK mit dem im maskenprogrammierten Festwertspeicher **32** der Chipkarte **14** abgelegten Freigabeschlüssel ENK' verglichen. Wenn auch dieser Vergleich positiv ausfällt, so wird das weitere Laden der Initialisierung freigegeben; andernfalls wird der Vorgang abgebrochen. In Ausführungsalternativen können die Schritte **66** und **68** auch in anderer Reihenfolge ausgeführt werden.

[0043] Bei einer Fortsetzung des Initialisierungsvorgangs empfängt die Chipkarte **14** in Schritt **70** die verschlüsselten Initialisierungsdaten EIND. Diese Daten werden in Schritt **72** entschlüsselt, wobei der Ladeschlüssel LDK des berechneten Authentisierungswerts AV zur Entschlüsselung eingesetzt wird. Das in Schritt **72** angewendete Entschlüsselungsverfahren kann ferner von einem oder mehreren der Initialisierungsparameter INP anhängen; beispielsweise kann je nach dem Parameterwert entweder DES oder TRIPLE DES eingesetzt werden. Natürlich muß das Entschlüsselungsverfahren in Schritt **72** mit dem in Schritt **42** (**Fig. 2**) zur Verschlüsselung verwendeten Verfahren übereinstimmen. Als Ergebnis des Entschlüsselungsschritts **72** erhält die Chipkarte **14** die Initialisierungsdaten IND, die in Schritt **74** in den nichtflüchtigen Speicher **30** geschrieben werden.

[0044] Zur Vereinfachung der Darstellung sind in **Fig. 3** die Schritte **70** bis **74** sequentiell dargestellt, während in

dem hier beschriebenen Ausführungsbeispiel diese Schritte ineinander verzahnt ablaufen, um den knappen Speicherplatzgegebenheiten der Chipkarte **14** zu genügen

[0045] Nach dem Laden der Initialisierungsdaten IND in den nichtflüchtigen Speicher **30** erfolgt in Schritt **76** auf an sich bekannte Weise eine weitere Integritätsprüfung mittels einer weiteren, kryptographischen Prüfsumme. Fällt diese Integritätsprüfung positiv aus, wird die Initialisierung in Schritt **78** aktiviert. Dabei werden im hier beschriebenen Ausführungsbeispiel ein oder mehrere Initialisierungsparameter INP eingesetzt, um die Initialisierung abschließend zu parametrisieren. Beispielsweise kann vorgesehen sein, durch die Initialisierungsparameter INP eine Auswahl unter mehreren, im Festwertspeicher **32** befindlichen Algorithmen zur Authentifizierung im GSM-System zu treffen.

Patentansprüche

1. Verfahren zum Einlesen von Initialisierungsdaten (IND) in eine Chipkarte (**14**), mit den durch die Chipkarte (**14**) ausgeführten Schritten:
   - Empfangen eines verschlüsselten Authentisierungswerts (EAV),
   - Entschlüsseln des verschlüsselten Authentisierungswerts (EAV), um zumindest einen Freigabeschlüssel (ENK) zu erhalten,
   - Überprüfen, ob der erhaltene Freigabeschlüssel (ENK) mit einem auf der Chipkarte (**14**) gespeicherten Freigabeschlüssel (ENK') übereinstimmt,
   - falls eine Übereinstimmung der Freigabeschlüssel (ENK, ENK') vorliegt, Empfangen und Einschreiben der Initialisierungsdaten (IND) in einen nichtflüchtigen Speicher (**30**) der Chipkarte (**14**)

2. Verfahren nach Anspruch 1,
bei dem durch das Entschlüsseln des verschlüsselten Authentisierungswerts (EAV) ferner zumindest ein Ladeschlüssel (LDK) erhalten wird, und
bei dem die Initialisierungsdaten (IND) als verschlüsselte Initialisierungsdaten (EIND) von der Chipkarte (**14**) empfangen und dort mit dem Ladeschlüssel (LDK) entschlüsselt werden

3. Verfahren nach Anspruch 1 oder Anspruch 2, bei dem durch das Entschlüsseln des verschlüsselten Authentisierungswerts (EAV) ferner zumindest ein Initialisierungsparameter (INP) erhalten wird, der den weiteren Einlese- und/oder Initialisierungsvorgang und/oder die spätere Funktionsweise der Chipkarte (**14**) beeinflußt.

4. Verfahren nach den Ansprüchen 1, 2 und 3, bei dem der Freigabeschlüssel (ENK) und/oder der Ladeschlüssel (LDK) und/oder der mindestens eine Initialisierungsparameter (INP) durch eine kryptographische Prüfsumme (CCS) abgesichert sind, wobei die kryptographische Prüfsumme (CCS) aus dem Authentisierungswert (AV) ableitbar ist.

5. Chipkarte mit einem Mikrocontroller (**26**), einem Festwertspeicher (**32**) und einem nichtflüchtigen Speicher (**30**), die dazu eingerichtet ist, unter Steuerung des Mikrocontrollers (**26**) ein Verfahren nach einem der Ansprüche 1 bis 4 auszuführen.

6. Verfahren zum Erzeugen eines Datensatzes (DS) für die Initialisierung einer Chipkarte (**14**), mit den Schritten:
   - Erzeugen eines Authentisierungswerts (AV), aus dem zumindest ein Freigabeschlüssel (ENK) ableitbar ist,
   - Verschlüsseln des Authentisierungswerts (AV) mit einem Authentisierungswertschlüssel (AVK), um einen verschlüsselten Authentisierungswert (EAV) zu erhalten,
   - Aufnehmen des verschlüsselten Authentisierungswerts (EAV) in den Datensatz (DS) und
   - Aufnehmen von unverschlüsselten oder verschlüsselten Initialisierungsdaten (IND, EIND) in den Datensatz (DS)

7. Verfahren nach Anspruch 6,
bei dem ein Ladeschlüssel (LDK) erzeugt wird und
bei dem die Initialisierungsdaten (IND) mit dem Ladeschlüssel (LDK) verschlüsselt und als verschlüsselte Initialisierungsdaten (EIND) in den Datensatz (DS) aufgenommen werden

8. Verfahren nach Anspruch 6 oder Anspruch 7, bei dem der Authentisierungswert (AV) derart erzeugt wird, daß aus ihm ferner zumindest ein Initialisierungsparameter (INP) ableitbar ist, der den späteren Einlese- und/oder Initialisierungsvorgang und/oder die spätere Funktionsweise der Chipkarte (**14**) beeinflußt.

9. Verfahren nach den Ansprüchen 6, 7 und 8, bei dem der Freigabeschlüssel (ENK) und/oder der Ladeschlüssel (LDK) und/oder der Initialisierungsparameter (INP) im Authentisierungswert (AV) durch eine kryptographische Prüfsumme (CCS) abgesichert sind, wobei der Authentisierungswert (AV) derart erzeugt wird, daß aus ihm die kryptographische Prüfsumme (CCS) ableitbar ist.

10. Computerlesbarer Datenträger mit einem Datensatz (DS), der durch ein Verfahren nach einem der Ansprüche 6 bis 9 erzeugbar ist oder erzeugt worden ist.

11. Verfahren zum Initialisieren einer Chipkarte (**14**), mit den Schritten:
   - Erzeugen eines Datensatzes nach einem Verfahren gemäß einem der Ansprüche 6 bis 9 in einer Herstellerstation (**10**),
   - Übertragen des Datensatzes (DS) zu einer Bearbeitungsstation (**12**),
   - Einlesen des Datensatzes (DS) in die Chipkarte (**14**) nach einem Verfahren gemäß einem der Ansprüche 1 bis 4

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 101 42 351 A1
Int. Cl.[7]: G 06 K 19/073
Offenlegungstag: 20. März 2003

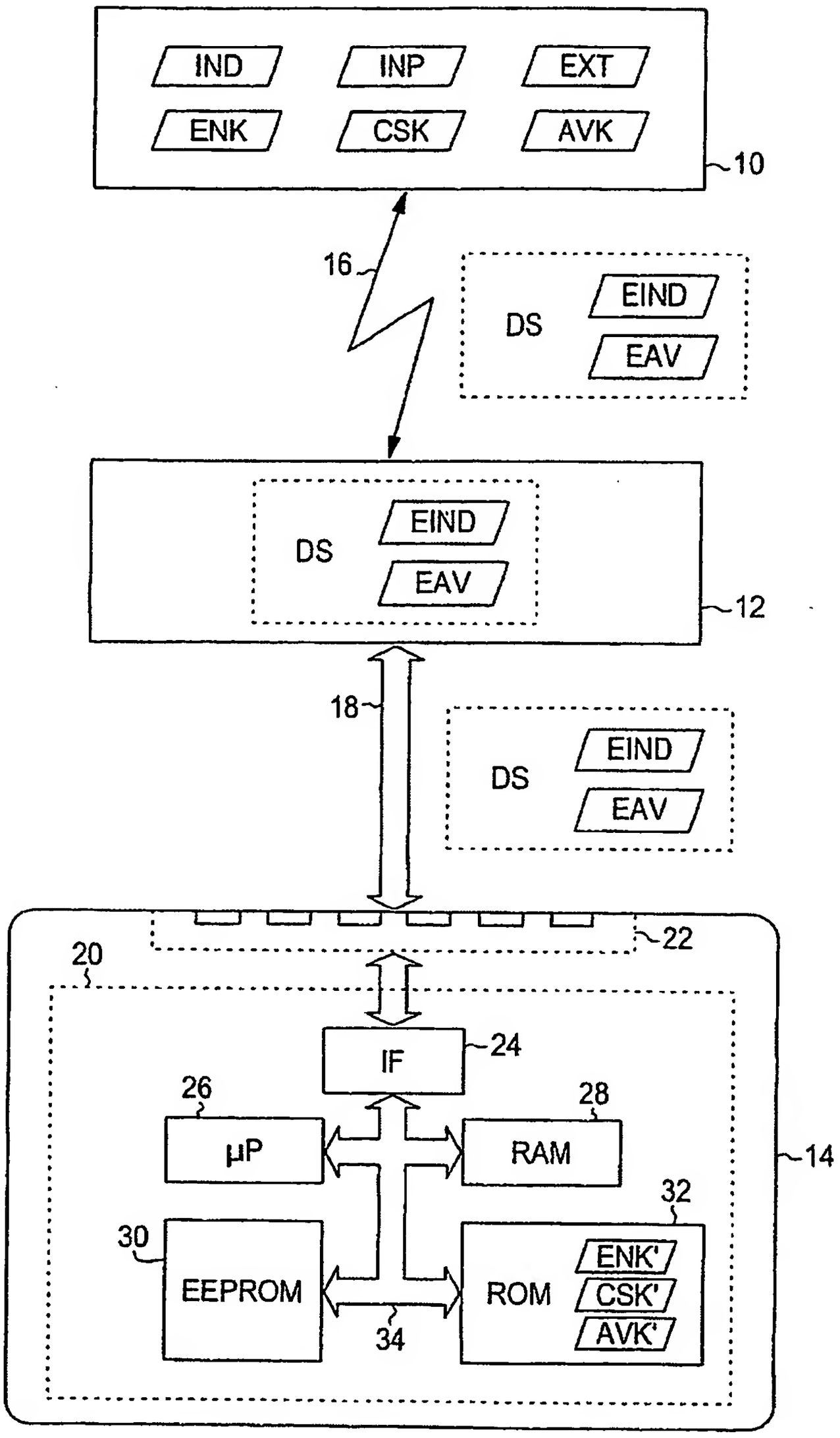


Fig. 1

Nummer: DE 101 42 351 A1
Int. Cl.[7]: G 06 K 19/073
Offenlegungstag: 20 März 2003

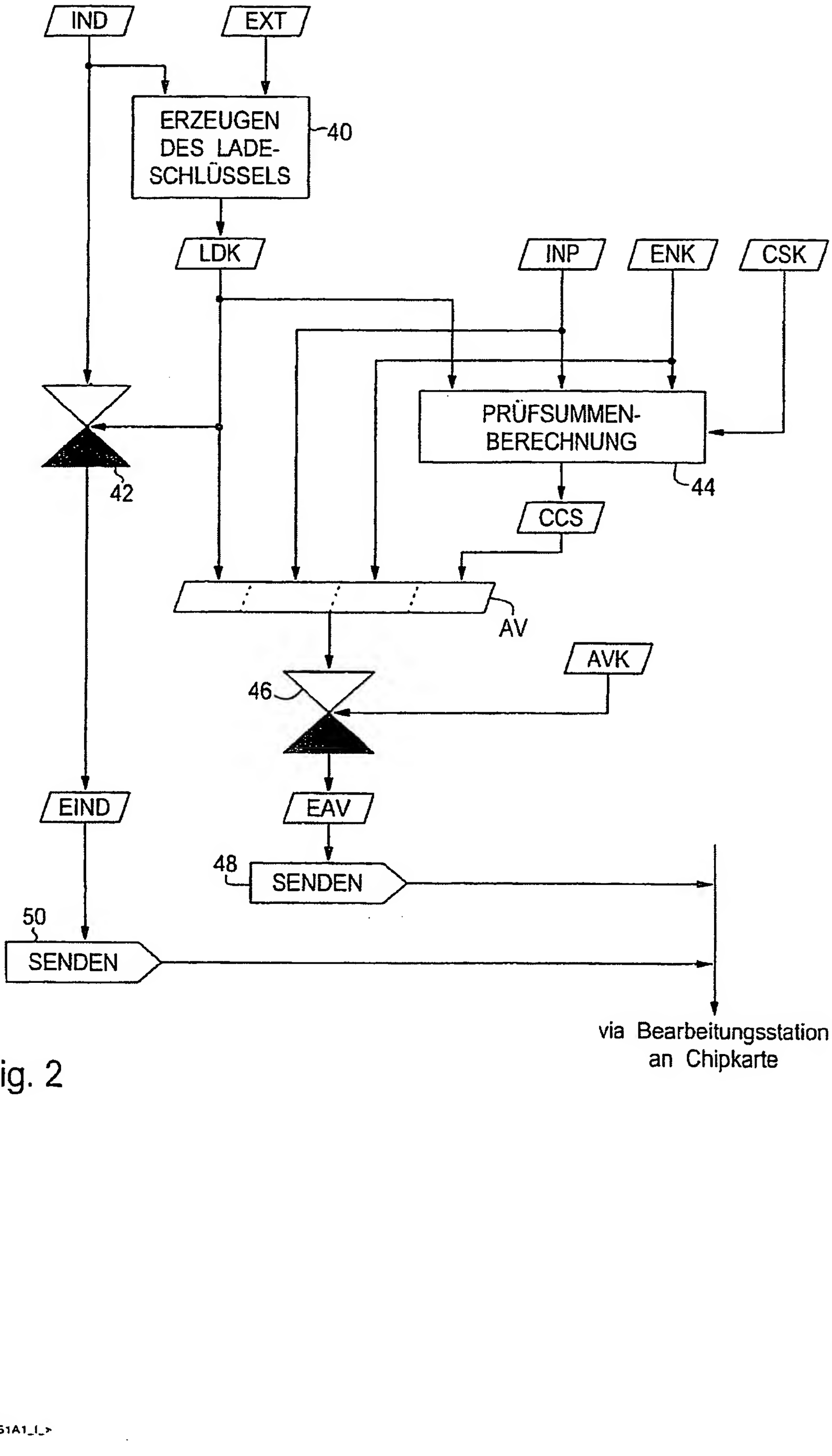


Fig. 2

Nummer: DE 101 42 351 A1
Int. Cl.[7]: G 06 K 19/073
Offenlegungstag: 20. März 2003

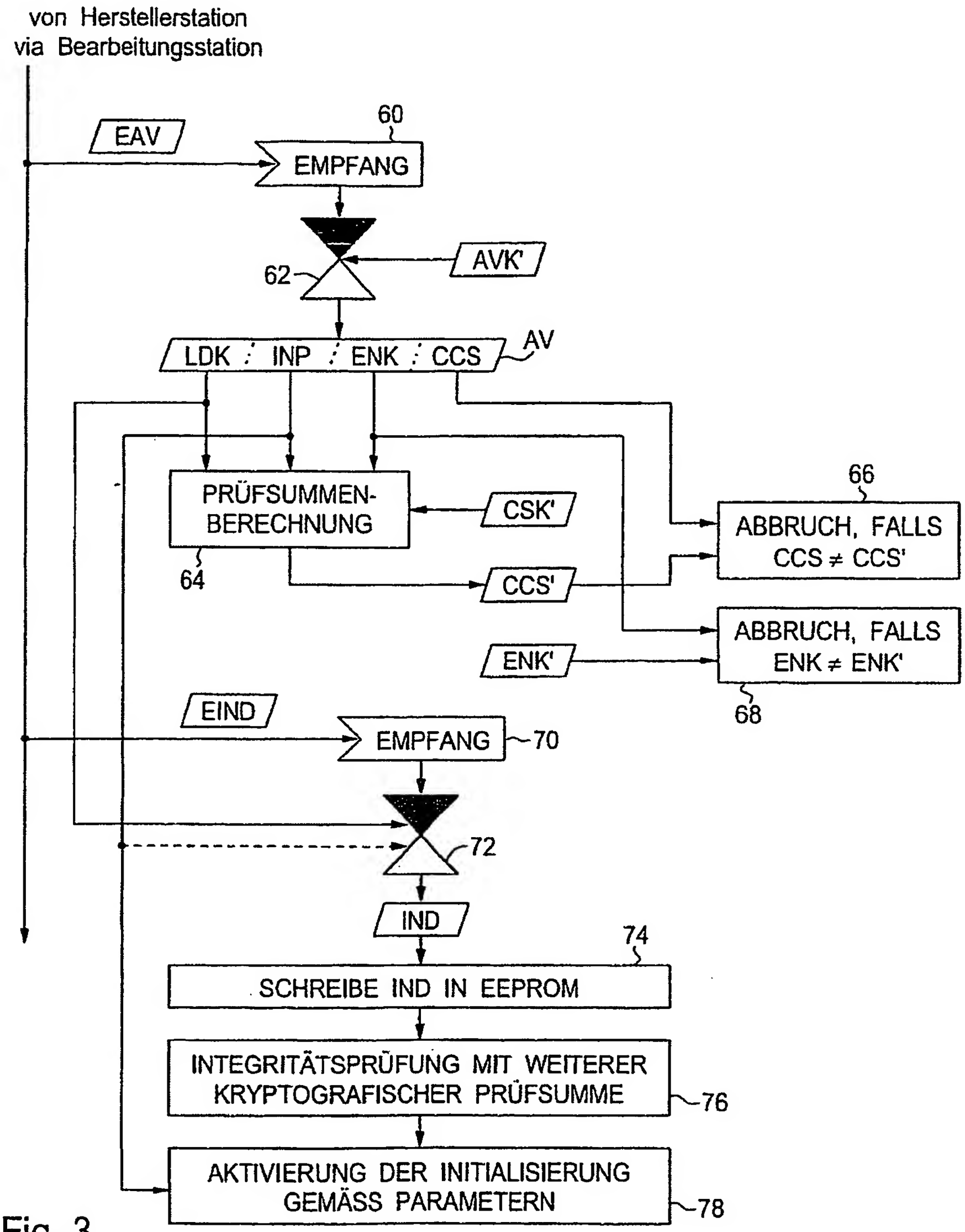


Fig. 3